CLAIMS

What is claimed is:

1. A method for capturing illegal and undesired behavior for network components and for interactions between components comprising:

specifying one or more states and state transitions for one or more components or interactions between two or more components, wherein specifying includes specifying at least one composite state transition; and

if a said state or state transition occurs, generating a notification corresponding to the specified state or state transition.

2. The method recited in claim 1, wherein said states are specified based on thresholds.

3. The method recited in claim 1, wherein the notification is an event.

4. The method recited in claim 1, wherein a state or state transition is a state or state transition of a component, and wherein the step of generating the notification comprises generating the notification by the component.

5. The method recited in claim 1, wherein if the state or state transition relates to an interaction between components, and wherein the notification is generated by at least one of the components involved in the interaction between the components.

6. The method recited in claim 1, further comprising the step of:

reporting the notification to a network management system.

7. The method recited in claim 1, further comprising the step of:

detecting whether a state or state transition has occurred; and

wherein if said step of detecting detects that a state or state transition has occurred, said notification is generated in response to said step of detecting.

8. The method recited in claim 7, wherein, the step of detecting is performed by an agent.

9. The method recited in claim 8, wherein the agent is a dedicated agent.

10. The method recited in claim 1, further comprising the step of polling said components to determine whether a state or state transition has occurred.

11. The method recited in claim 1, wherein the step of specifying one or more states and state transitions comprises specifying illegal states.

12. The method recited in claim 1, wherein the step of specifying one or more states and state transitions comprises specifying undesired states.

13. The method recited in claim 1, wherein the step of specifying one or more states and state transitions comprises specifying illegal states and undesired states.

14. The method recited in claim 6, wherein detecting whether a state or state transition has occurred comprises determining whether a component or component interaction has entered an illegal or undesired state.

15. The method recited in claim 11 wherein an authorization violation and an authentication forgery are defined as illegal states.

16. The method recited in claim 12, wherein a nongracefully QoS degradation is defined as an undesired state.

17. The method recited in claim 1, further comprising the step of examining multiple notifications to deduce trends regarding the network.

18. The method recited in claim 17, wherein the step of examining multiple notifications comprises examining notifications for stable-behavior in a threshold value.

19. The method recited in claim 17, wherein the step of examining multiple notifications comprises examining notifications for increases or decreases in a threshold value.

20. A system for capturing illegal and undesired behavior for network components and for interactions between components, the system comprising:

one or more network components configured to spontaneously generate notifications upon the occurrence of specified states and state transitions, including one or more composite state transitions; and a network management system configured to receive said spontaneously generated notifications.

21. The system of claim 20, further comprising:

an agent configured to detect the generation of notifications by the network components, and configured to report detected notifications to said network management system.

22. The system of claim 20, further comprising:

a state table configured to store said specified states and state transitions, including composite state transitions.

23. The system of claim 21, wherein the state table is in a network management system.

24. The system of claim 21, wherein the state table is in a network component.

25. The system of claim 22, wherein the agent is further configured to examine one or more conditions of one or more network components and to query the state table to determine whether the one or more conditions represents an illegal or undesired state.

26. The system of claim 22, wherein the agent is further configured to examine one or more transitions relating to one or more network components and to query the state table to determine whether the one or more transitions represents an illegal or undesired transition.

27. A system for capturing illegal and undesired behavior for network components and for interactions between components comprising:

one or more network components;

an agent configured to examine said network components to determine whether specified states or state transitions, including composite state transitions, have occurred, wherein the agent is configured to generate notifications upon a determination that a specified state or state transition has occurred, and wherein the agent is configured to report detected notifications to said network management system; and

a network management system configured to receive reports of said generated notifications.

28. The system of claim 27, further comprising:

a state log configured to store said specified states and state transitions, including composite state transitions.

29. A computer-readable medium carrying one or more sequences of instructions for capturing illegal and undesired behavior for network components and for interactions between components, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

specifying one or more states and state transitions for one or more components or interactions between two or more components, wherein specifying includes specifying at least one composite state transition; and

if a said state or state transition occurs, generating a notification corresponding to the specified state or state transition.

30. A computer-readable medium as recited in Claim 29, wherein said states are specified based on thresholds.

31. A computer-readable medium as recited in Claim 29, wherein said notifications are events.

32. A computer-readable medium as recited in Claim 29, wherein a state or state transition is a state or state transition of a component, and wherein the step of generating a notification comprises generating the notification by the component.

33. A computer-readable medium as recited in Claim 29, wherein if the state or state transition relates to an interaction between components, and wherein the notification is generated by at least one of the components involved in the interaction between the components.

34. A computer-readable medium as recited in Claim 29, wherein the instructions for carrying out the step of creating and storing first information further comprise instructions for carrying out the step of:

reporting the notification to a network management system.

35. A computer-readable medium as recited in Claim 29, wherein the instructions for carrying out the step of creating and storing first information further comprise instructions for carrying out the steps of:

detecting whether a state or state transition has occurred; and wherein if said step of detecting detects that a state or state transition has occurred, said notification is generated in response to said step of detecting.

36. A computer-readable medium as recited in Claim 35, wherein the step of detecting is performed by an agent.

37. A computer-readable medium as recited in Claim 36, wherein the agent is a dedicated agent.

38. A computer-readable medium as recited in Claim 29, wherein the instructions for carrying out the step of creating and storing first information further comprise instructions for carrying out the step of:

polling said components to determine whether a state or state transition has occurred.

39. A computer-readable medium as recited in Claim 29, wherein the step of specifying one or more states and state transitions comprises specifying illegal states.

40. A computer-readable medium as recited in Claim 29, wherein the step of specifying one or more states and state transitions comprises specifying undesired states.

41. A computer-readable medium as recited in Claim 29, wherein the step of specifying one or more states and state transitions comprises specifying illegal states and undesired states.

42. A computer-readable medium as recited in Claim 35, wherein detecting whether a state or state transition has occurred comprises determining whether a component or component interaction has entered an illegal or undesired state.

43. A computer-readable medium as recited in Claim 39, wherein an authorization violation and an authentication forgery are defined as illegal states.

44. A computer-readable medium as recited in Claim 40, wherein a nongracefully QoS degradation is defined as an undesired state.

45. A computer-readable medium as recited in Claim 29, wherein the instructions for carrying out the step of creating and storing first information further comprise instructions for carrying out the step of examining multiple notifications to deduce trends regarding the network.

46. A computer-readable medium as recited in Claim 45, wherein the step of examining multiple notifications comprises examining notifications for stable-behavior in a threshold value.

47. A computer-readable medium as recited in Claim 45, wherein the step of examining multiple notifications comprises examining notifications for increases or decreases in a threshold value.